



TITLE:

# 円分体のideal類群と保型形式及び K群について(代数的整数論)

AUTHOR(S):

栗原, 将人

---

CITATION:

栗原, 将人. 円分体のideal類群と保型形式及びK群について(代数的整数論). 数理解析研究所講究録 1991, 759: 66-75

ISSUE DATE:

1991-06

URL:

<http://hdl.handle.net/2433/82198>

RIGHT:

# 円分体の ideal 類群と保型形式及び $K$ 群について

都立大・理 栗原 将人 (Masato Kurihara)

円分体は近代的整数論の発祥の地であり古い歴史を持つが、その理論は 発展の可能性を秘めた様々な理論の端的な例を孕之ると同時に、それ自体の美しさにより、で今でも独特の位置を占めている<sup>(注)</sup>。ここでは岩澤理論と密接に関連する円分体の  $p$  分体のイデアル類群の  $p$ -part の構造について主に 2 つの方向から考えていく。すなわち円分体の  $p$  分体の類群の構造についての有名な予想と  $\mathbb{Z}$  の  $K$  群、及び level 1 保型形式との関係について述べる。更に円分体の  $p$  分体という有理数体の拡大体の話を下位の体  $\mathbb{Q}$  (あるいは  $\mathbb{Z}$ ) に落とした話であることに注意しておく。

1. 奇素数 (非正則素数)  $p$  に対して  $K = \mathbb{Q}(\mu_p)$  を円分体の  $p$  分体,  $\Delta = \text{Gal}(K/\mathbb{Q})$  をその Galois 群,  $A$  を  $K$  のイデアル類群の  $p$ -Sylow 部分群とする。  $\Delta$  の位数は  $p-1$  と素だから  $A$  は  $\Delta$  の

作用によ, 2

$$A = \bigoplus_{i \in \mathbb{Z}/(p-1)\mathbb{Z}} A^{[i]}$$

と分解される.  $\omega: \Delta = (\mathbb{Z}/p)^{\times} \rightarrow \mathbb{Z}_p^{\times}$  は Teichmüller 指標.

とし  $A^{[i]} = \{x \in A \mid \sigma(x) = \omega^i(\sigma)x \text{ for all } \sigma \in \Delta\}$  とある.

$A^{[0]} = A^{[1]} = 0$  はすぐに分かる. また Mazur Wiles によ, 2

証明された Iwasawa's main conjecture の帰結とし  $j \not\equiv 1 \pmod{p-1}$  なる奇数  $j$  に対し

$$\text{ord}_p \# A^{[j]} = \text{ord}_p L(0, \omega^j) = \text{ord}_p B_{1, \omega^j}$$

であることが知られている.  $L(s, \omega^j)$  は Dirichlet  $L$

関数,  $B_{1, \omega^j}$  は generalized Bernoulli number である. なお最近

Kolyvagin は Gauss 和の Euler system を使, 2 上の事実の main

conjecture を証明した (偶数  $i$  に対して  $A^{[i]}$

の位数を円単数を使, 2 書くことが出来る.) しかしこのよう

な zeta 関数の特殊値との関係だけからでは  $A^{[i]}$  の構造はわか

らない.  $A^{[i]}$  の構造についてはやや樂觀的な次のような予想

がある.

予想 1. (Kummer Vandiver) 偶数  $i$  に対して  $A^{[i]} = 0$

予想 2.  $j \in j \not\equiv 1 \pmod{p-1}$  なる奇数とすると

$$A^{[j]} \simeq \mathbb{Z}_p / B_{1, \omega^j} \mathbb{Z}_p$$

よく知られているように予想 1 には理論的根拠は何もない.

ただこの予想が正しいとすると円分体論は著しく簡潔になるのである。dualityにより偶数  $i$  に対する予想 1 は  $j=1-i$  に対する予想 2 と導く。

岩澤理論との関係を一言述べておこう。 $L/\mathbb{Q}(\mu_{p^\infty}) \in \mathbb{Q}(\mu_{p^\infty})$  の最大不分岐 abel 拡大とする。main conjecture の述べるところは  $\text{Gal}(L/\mathbb{Q}(\mu_{p^\infty}))^-$  の“特性多項式”が  $p$  進  $L$  関数であるということである。予想 2 が正しいければ特性多項式がわかるだけでなく  $\text{Gal}(L/\mathbb{Q}(\mu_{p^\infty}))^-$  は  $\mathbb{Z}_p[[\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})]]/(p \text{ 進 } L)$  と同型になる。以上の予想及び関連する事柄については岩澤先生の [1] にまとめられている。筆者の円分体論への興味はこのときの数理論における岩澤先生の簡潔にして感銘深い講演から始まった。この機会に岩澤先生並びにそのシンポジウムを組織された佐武先生、森田先生に感謝の気持ちを表したく思います。

2.  $\mathbb{Z}$  は有理整数環,  $K_*(\mathbb{Z}) \in \mathbb{Z}$  の  $K$  群とする。  $K_n(\mathbb{Z})$  ( $n \geq 0$ ) に関することは  $K$  理論の最も基本的な問題だと思われるが、現状ではその有限生成 abel 群であること (Quillen), rank の計算 (Borel),  $n \leq 5$  のときの結果 (Lee Szczarba 等) くらいしか知られていない。ここでは  $K_n(\mathbb{Z})$  の torsion part  $K_n(\mathbb{Z})_{\text{tors}}$  に対して次のように予想する。

予想 3  $K_n(\mathbb{Z})_{\text{tors}}$  は 2-torsion を除いて巡回群である。

予想3は予想2を導く。もっと詳しく

予想4.  $n \geq 1$  に対し

$$1) \quad K_{4n}(\mathbb{Z}) \sim 0$$

$$2) \quad K_{4n+1}(\mathbb{Z}) \sim \mathbb{Z}$$

$$3) \quad K_{4n+2}(\mathbb{Z}) \sim \mathbb{Z}/N_{2n+2}\mathbb{Z}$$

$$4) \quad K_{4n+3}(\mathbb{Z}) \sim \mathbb{Z}/D_{2n+2}\mathbb{Z}$$

ここに  $A \sim B$  は 2-torsion を除く同型を表す。また  $N$  は正の偶数としたとき  $N_R, D_R$  は

$$\zeta(1-R) = (-1)^{\frac{R}{2}} \frac{N_R}{D_R} \quad (N_R, D_R) = 1$$

なる自然数。  $\zeta(s)$  は Riemann zeta 関数。

定理1. (1) 予想4.1)は予想1, 予想2を導く。より正確には

$K_{4n}(\mathbb{Z})/p^4$  ( $K_{4n}(\mathbb{Z})$  の  $p$ -Sylow 部分群)  $= 0$  であるとする。

$A^{[-2n]} = 0$  であり  $A^{[2n+1]} \simeq \mathbb{Z}_p / B_{1, \omega^{2n+1}} \mathbb{Z}_p$  となる。

(2) 予想4.3)は予想2,  $j = -2n-1$  を導く。

系.  $A^{[p-3]} = 0, A^{[3]} \simeq \mathbb{Z}_p / B_{1, \omega^3} \mathbb{Z}_p$ .

これは Lee Szczarba Soulé の定理  $K_4(\mathbb{Z})/p^4 = 0$  ( $p \geq 5$ ) と上の定理1(1)から帰結である。

定理1の証明は Chern class  $K_{2r-2}(\mathbb{Z}) \rightarrow H_{\text{ét}}^2(\mathbb{Z}[p], \mathbb{Z}_p(r))$  の全

射性と同型

$$A^{[1-r]}/p \simeq H_{\text{ét}}^2(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p(r))$$

による。

3. 上の系の応用をいくつか述べる。まず  $A^{[p-3]} = 0$  なる伊原先生 [2] の Th. 6 の条件はすべて正しい。[2] の元と行った [3] なるいくつかの結果を述べよう。  $a \in 1 \leq a \leq p-2$  なる整数とし  $J$  は curve  $y^p = x^a(1-x)$  の Jacobian,  $J(\mathbb{Q}(M_p))$  は  $J$  の  $\mathbb{Q}(M_p)$  有理点で位数が  $p$  中  $a$  元全体とする。  $\pi = 1 - \zeta_p$  ( $\zeta_p$ : 1 の原始  $p$  乗根),  $J[\pi^3]$  は  $J(\overline{\mathbb{Q}})$  の  $\pi^3$  等分点全体とする。(  $J$  は  $\mathbb{Z}[M_p]$  の CM を持つ。 ) [3] Th. 1 では  $J[\pi^3] \subset J(\mathbb{Q}(M_p))$  を示す述べた。  $A^{[p-3]} = 0$  なる

$$J(\mathbb{Q}(M_p)) \mid p^4 = J[\pi^3] (\simeq (\mathbb{Z}/p)^{\oplus 3})$$

がわかる。 Jacobi 和, 及び  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  の表現との関係について詳しくは [2] を見て頂きたい。

次に  $A^{[3]} \simeq \mathbb{Z}_p / B_{1, \omega^{-3}} \mathbb{Z}_p$  の応用について述べる。 Vandiver は Fermat の問題の第 1 の場合が誤, であるとする, つまり  $x^p + y^p = z^p$ ,  $p \nmid xyz$  なる自然数  $x, y, z$  が存在すると仮定すると  $p^2 \mid B_{(p-4)p+1}$  であることを示した。 一方 Kummer の合同式から  $B_{1, \omega^{-3}} \equiv -B_{(p-4)p+1} / ((p-4)p+1) \pmod{p^2}$  である。 従って, 2 元 Fermat の問題の第 1 の場合が誤, であるとする  $A^{[3]}$

は位数  $p^2$  の元を持つことになる。  $A$  の位数  $p^2$  の元を持つということ是非常に強い条件であり、そんな人今まで知られていない中ではこのような例は存在しない。今ある Fermat の問題の第 1 の場合と Bernoulli 数の関係については最近岩澤先生と藤崎先生が、と詳しく調べている。

4. 保型形式に話を移そう。  $k \in \mathbb{Z}$  の偶数とし、  $M_k$  を重  $k$  の  $SL_2(\mathbb{Z})$  に関する保型形式全体のなす空間、  $M_k^0$  を cusp forms 全体を表すことにする。  $T_k \in \text{End}(M_k^0)$  の部分環で  $\mathbb{Z}$  上 Hecke 作用素  $T_k$  たちで生成される環とする。  $T_k$  は  $\mathbb{Z}$  上 finite であり rank は  $\dim M_k^0$  に等しい。  $p \in p-1 > k$  なる素数とする。

$T_k \otimes \mathbb{Z}_p$  を考えるとこれは  $\mathbb{Z}_p$  上 finite であり局所環の直和になる。

予想 5.  $R \in T_k \otimes \mathbb{Z}_p$  の ordinary の local component の局所環とすると  $R$  は 1 次元の Gorenstein 環である。

ここに  $R$  の ordinary とは  $m_R \in R$  の極大 ideal としたとき  $T_p$  の  $R/m_R$  での像が 0 であることと定義する。  $R$  の 1 次元の Gorenstein 環であることは  $\text{Hom}(R, \mathbb{Z}_p)$  が  $R$  加群として  $R$  と同型であることと同値である。  $f = \sum_{n \geq 1} a_n q^n \in \text{mod } p \text{ eigenform}$   $a_1 = 1, a_n \in F$  ( $F$ : 有限体  $\mathbb{F}_p$ ) とする。  $f$  に伴う表現を

$\rho_f: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(F)$  とする。すなわち  $\rho_f$  は semi simple で  
 $\text{tr}(\rho_f(\text{Frob}_\ell)) = a_\ell$ ,  $\det(\rho_f(\text{Frob}_\ell)) = \ell^{k-1}$  ( $\ell \neq p$ )。  $\rho_f$  は既約であ  
 る。  $f$  に対応する  $\mathbb{T}_k \otimes \mathbb{Z}_p$  の local component  $\mathbb{T}_f$  について上  
 の予想は正しい。

予想 5 は予想 2 に導く。正確に述べる。今  $A^{[1-k]} \neq 0$  と  
 仮定する。従って  $p \mid B_k$  とする。このとき Eisenstein series  
 $G_k = \frac{1}{2} S(1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$  は mod  $p$  cusp form になる。  $\mathbb{T}^E$   
 に対応する  $\mathbb{T}_k \otimes \mathbb{Z}_p$  の local component とする。すなわち  $\mathbb{T}^E \in$  極大  
 ideal  $\mathfrak{m}$  の

$$\mathfrak{m} = (p, T_\ell - (1 + \ell^{k-1}), \dots) \quad (\ell \text{ は } k \text{ と } n \text{ の素数でない})$$

で与えられる component とする。

定理 2. (1)  $\mathbb{T}^E$  は Gorenstein である。  $j=1-k$  に対する予想  
 2 は正しい。

(2)  $\mathcal{I} \in T_\ell - (1 + \ell^{k-1})$  ( $\ell$ : 素数) によって生成される  $\mathbb{T}^E$  の  
 ideal (Eisenstein ideal) とする。  $p^n \parallel B_k$  とすると  $\mathbb{T}^E/\mathcal{I} \simeq$   
 $\mathbb{Z}/p^n$  であり、  $\mathcal{I}/\mathcal{I}^2$  の位数  $p^n$  の元を持つのは  $j=1-k$  に対する  
 予想 2 は正しい。

特に上の  $\mathcal{I}$  の主 ideal であるのは予想 2 から導かれることである。  
 また  $d_{\mathbb{T}_k/\mathbb{Z}} \in \mathbb{T}_k$  の判別式としたとき、  $p \nmid d_{\mathbb{T}_k/\mathbb{Z}}$  であ  
 るのは  $\mathbb{T}^E \simeq \mathbb{Z}_p$  であるから予想 2 は正しい。また  $G_k \bmod p$  の



標数  $0$  の normalized eigen cusp form  $f$  を持つ  $n \geq 2$  以下し  
 れば  $\text{rank}_{\mathbb{Z}_p} \mathbb{T}^E \leq 2$  である。やはり予想 2 が正し  
 いことになる。

逆も成り立つ。

定理 3.  $i = 2 - k$  について予想 1 を仮定する。このとき  
 次の同値。

- (1)  $\mathbb{T}^E$  は Gorenstein
- (2)  $\mathfrak{A}$  は  $\mathbb{T}^E$  の主 ideal.
- (3)  $\mathfrak{A}/\mathfrak{A}^2$  は位数  $p^n$  の元を持つ. ( $p^n \parallel B_E$ )
- (4)  $j = 1 - k$  に対して予想 2 が正しい。

特に予想 1 (Vandiver 予想) が一般に正しいければ Eisenstein ideal  
 $\mathfrak{A}$  は主 ideal である。

重さ 2, 指標  $\omega^{k-2}$  の  $\Gamma_1(p)$  に関する保型形式に対しても同様  
 なことはできる。

5. Ribet は [4] で  $p$ -分体に関する結果を得るために保型形式  
 に伴う Galois 表現を効果的に用いた。これはその後  $n$  種の  
 の議論の出発点となり、たが、ここで  $n$  の定理を得るために  
 保型形式に伴う  $p$ -進表現, すなわち étale cohomology

$$W = H_{\text{par}}^1(M_N \otimes \overline{\mathbb{Q}}, \text{Sym}^{k-2} R_{f*}^1 \mathbb{Z}_p(k-1))^{GL_2(\mathbb{Z}_N)} \quad (M_N: \text{level } \Gamma(N) \text{ を持つ})$$

楕円曲線の moduli space,  $f$ : universal elliptic curve) の  $\mathbb{T}^E$  component  $W^E$  を考へる。ここでは定理 2. (1) の証明の概略を与へることにする。 $\mathbb{T}^E$  は Gorenstein といふことは  $W^E$  から

$\rho_E: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{T}^E)$  なる 2 次元表現であることを見保証する。これは  $p$  を外で不台段である。今  $I \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  の  $p$  での積性群とするとき上の表現の  $I$  への制限は  $\begin{pmatrix} \chi^{p-1} & * \\ 0 & 1 \end{pmatrix}$

$\chi$ : cyclotomic character となり、 $\chi$  である。(ここまでは保型形式に伴う  $p$  進表現の一般論) さて Eisenstein ideal  $\mathfrak{I}$  に対し

$$\rho_E \bmod \mathfrak{I}: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{T}^E/\mathfrak{I}) \simeq \text{GL}_2(\mathbb{Z}/p^n)$$

を考へると  $\rho_E$  の分解群  $D$  への制限は split  $\begin{pmatrix} \chi^{p-1} & 0 \\ 0 & 1 \end{pmatrix}$  としてあり、さらに  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  全体の表現として  $\begin{pmatrix} \chi^{p-1} & 0 \\ * & 1 \end{pmatrix}, * \in p(\mathbb{Z}/p^n)$

なる型であることを示せる。(ただし正確には  $\mathbb{T}^E \neq \mathbb{Z}_p$  と仮定した。 $\mathbb{T}^E = \mathbb{Z}_p$  となることは、簡単に (その必要はないと思うのだが) lattice をとり直せば上のようになる。) 従って

$(\rho_E \bmod \mathfrak{I}) \otimes \chi^{1-p}$  は  $\text{Ext}_{\mathbb{Z}[\frac{1}{p}]}^1(\mathbb{Z}/p^n, \mathbb{Z}/p^n(1-p)) \simeq H_{\text{et}}^1(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p^n(1-p))$  の元で  $p$  での分解群に制限すると trivial になり、したがって位数  $p^n$  の元を与へる。つまり

$$\text{Ker}(H_{\text{et}}^1(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p^n(1-p)) \rightarrow H^1(\mathbb{Q}_p, \mathbb{Z}/p^n(1-p)))$$

の位数  $p^n$  の元を与へることになる。Tate Poitou の duality により、 $\rho_E$  上の群は  $H_{\text{et}}^2(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p^n(p))$  の双対と同型。一方 Iwasawa's main conjecture により  $\# H_{\text{et}}^2(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p^n(p)) = p^n$  である。従って

$H_{\text{ét}}^2(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p^n(k)) \simeq \mathbb{Z}/p^n$  であらねばならず、これは  
 $H_{\text{ét}}^2(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p(k)) \simeq \mathbb{Z}/p$  と等しく、 $n=1$  と  $2$  で述べた同型  
 $A^{[1-k]}/p \simeq H_{\text{ét}}^2(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}/p(k))$  と  $A^{[1-k]}$  の巡回群であること  
 から従うのである。

## References

- [1] 岩澤健吉, 円分体に関するいくつかの問題, 数理論講究  
録 658, p. 43 - 55
- [2] Y. Ihara, Profinite braid groups, Galois representations and  
Complex multiplications, Ann. of Math. 123, p. 43 - 106
- [3] R. Greenberg, On the Jacobian variety of some algebraic curves,  
Compos. Math. 42, p. 345 - 359
- [4] K. Ribet, A modular construction of unramified  $p$ -extensions  
of  $\mathbb{Q}(\mu_p)$ , Invent. math. 34, p. 151 - 162

(注) この書き出した文章の一部は K. Iwasawa Ann. of Math. (1959) p. 530-561 に引用されて頂いた。